UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,060	01/28/2002	Scott A. Vanstone	13889	5472

293 7590 05/04/2005

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave.
Suite 406
Alexandria, VA 22314

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/056,060	VANSTONE ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-39 and 41-47* is/are rejected.

7)☐ Claim(s) *40 and 48* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 June 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/015,338.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 31-48 are pending.

2. Claims 1-30 were canceled in the amendment filed on September 15, 2005.

3. Claims 31-48 were added in the amendment.

Response to Amendment

4. The double patenting rejection of claims 1-30 are withdrawn as the claims were canceled and replaced by new claims 31-48.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 31, 32, 34, 36-38, 42 and 44-46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 36-38 and 44-46 recite the limitation "said shared key". There is insufficient antecedent basis for this limitation in the claims.

8. Claims 31, 32, 34 and 42 recite the limitations "(d)", "(k)" and "(Qb)". It is not clear if these terms are recited to narrow the scope of the limitations.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. Claims 31-39 and 41-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Rueppel et al. USPN 5,600,725 (hereinafter Rueppel).

11. As per claim 31, Rueppel discloses a method of establishing a session key between a pair of correspondents in a data communication system, each of the correspondents sharing secret information (d) (col. 2:48-3:38; 6:1-9:4; 8:18-23, "u" var; figure 3), the method comprising the steps of:

a. one of the correspondents generating additional secret information (k) and deriving therefrom a session key (6:9-10, 29-35);

b. the one of the correspondents transferring the additional secret information (k) to the other of the correspondents (6:38-41); and

c. the other of the correspondents using the secret information (d) and the additional secret information (k) to generate a session key (6:45-7:10).

The aforementioned cover the limitations of claim 31.

12. As per claim 32, the rejection of claim 31 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the secret information (d) and the additional secret information (k) are combined at the one correspondent in a signature algorithm to provide a first signature component and the additional secret information is obtained by the other correspondent by utilizing the secret information on the first signature component. Rueppel, 7:10; 8:1-15.

13. As per claim 33, the rejection of claim 32 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the first signature component includes public information associated with the other correspondent and the other correspondent utilizes the public information to obtain the additional secret information. Rueppel, col. 8:28-32.

14. As per claim 34, the rejection of claim 33 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the secret information (d) and the public information (Qb) are

combined in the signature algorithm and such combination is precomputed and stored by the one correspondent. Rueppel, col. 8:29-32.

15. As per claim 35, the rejection of claim 34 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the combination is the product of the secret information and the public information. Rueppel, col. 8:29-32.

16. As per claim 36, the rejection of claim 32 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the second signature component is derived from the shared key. Rueppel, col. 8:1-32.

17. As per claim 37, the rejection of claim 36 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, a portion of the shared key is utilized to provide the second signature component. Rueppel, col. 8:28-37.

18. As per claim 38, the rejection of claim 37 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the shared key represents the coordinates of a point on an elliptic curve and the portion is one of the coordinates. Rueppel, col. 8:28-37.

19. As per claim 39, the rejection of claim 37 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the portion is hashed by a secure hash function to provide the second signature component. Rueppel, col. 8:4.

20. As per claim 41, Rueppel discloses a method of establishing a session key between a first correspondent and a selected one of a plurality of second correspondents corrected to the first correspondent (fig. 3), the method comprising providing each of the second correspondents a respective secret information, storing each of the secret information at the first correspondent to associate each of the stored secret information with a respective correspondent (col. 8:1-38, "u" var), receiving from the selected one of the second correspondents a signature including a first component combining the secret information with additional secret information used by the selected one of the second correspondents to generate a session key (fig. 3, reference nos. 215, 220, 230, 240 and 245 and related text), retrieving the stored secret information associated with the selected one of the second correspondents and using the secret information and the additional information to generate a session key corresponding to the session key of the selected one of the second correspondents (fig. 3, 305, 310, 320, 330 and related text).

21. As per claim 42, the rejection of claim 41 under 35 U.S.C. 102(e) is incorporated herein. In addition, the secret information (d) and the additional secret information (k) are combined at the selected on of the second correspondents in a signature algorithm to provide a first signature component and the additional secret information is obtained by the first correspondent by utilizing the secret information on the first signature component. Rueppel, 7:10; 8:1-15.

22. As per claim 43, the rejection of claim 42 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the first signature component includes public information associated with the first correspondent and the first correspondent utilizes the public information to obtain the additional secret information. Rueppel, col. 8:28-32.

23. As per claim 44, the rejection of claim 42 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the second signature component is received by the first correspondent and is derived from the shared key. Rueppel, col. 8:1-32; fig. 3, reference no. 250.

24. As per claim 45, the rejection of claim 44 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, a portion of the shared key is utilized to provide the second signature component. Rueppel, col. 8:28-37.

25. As per claim 46, the rejection of claim 45 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the shared key represents the coordinates of a point on an elliptic curve and the portion is one of the coordinates. Rueppel, col. 8:28-37.

26. As per claim 47, the rejection of claim 45 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the portion is hashed by a secure hash function to provide the second signature component. Rueppel, col. 8:4.

Allowable Subject Matter

27. Claims 40 and 48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

28. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See enclosed PTO-892.

29. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
April 29, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100